БОЛЬШИЕ ВЫЗОВЫ

ВСЕРОССИЙСКИЙ КОНКУРС
НАУЧНО-ТЕХНОЛОГИЧЕСКИХ ПРОЕКТОВ

МГК 2021

Региональный трек
Всероссийского конкурса
научно-технологических проектов

«БОЛЬШИЕ ВЫЗОВЫ»

направление

Когнитивные исследования

название работы

Обучающая программа«Асимметричная криптосистема, основанная на задаче «рюкзака»

участник(и)

Капустин Владислав Игоревич

#большиевызовы
#мгк

mgk.olimpiada.ru

г. Москва
2021

Цель проекта:

создание достаточно простой и в то же время познавательной обучающей программы для эффективного изучения современных методов шифрования.

Задачи проекта:

- изучение всех компонентов информационной системы, в том числе и правовое обеспечение защиты информации, эксплуатации криптографических средств;
- разработка программного обеспечения;
- подготовка учебных материалов для проведения занятий по данной теме на основе кода программы.

Актуальность проекта:

Тема шифрования является наиболее популярной среди школьников разных возрастов. С каждым учебным годом рассматриваются все более и более сложные ее примеры, демонстрируя тем самым ее постоянную эволюцию.

Современное компьютерное шифрование использует последние достижения дискретной математики, алгебры, теории вероятностей, математической статистики, которые часто превышают уровень школьных знаний и являются предметом специального изучения в ВУЗах.

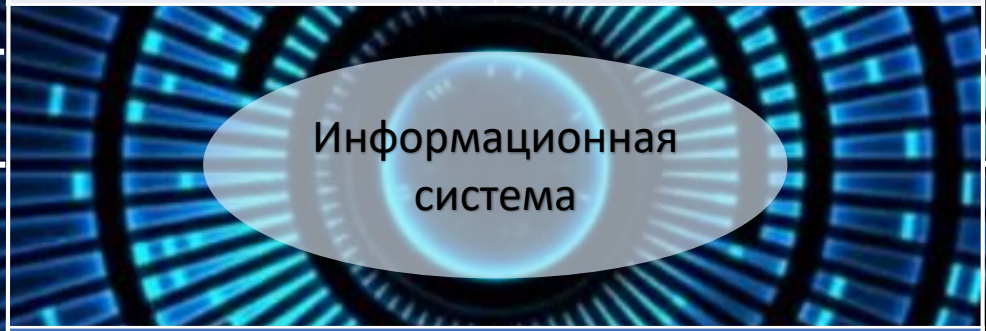
Поэтому создание обучающей программы, которая могла бы в доступной форме показать школьникам механизм шифрования, является весьма актуальной.

Дорожная карта проекта:

Направление работы, ключевые задачи \ Сроки	август 2020	сентябрь 2020	октябрь 2020	ноябрь 2020	декабрь 2020	январь 2021
Изучение методов шифрования, правовых основ защиты информации. Выбор метода шифрования, изучение математического аппарата.						
Анализ степени изученности и разработанности темы исследования. Постановка задач проекта.						
Разработка требований к обучающей программе. Выбор программной среды для реализации проекта.						
Разработка интерфейса и написание программного кода.						
Тестирование и модернизация программы.						
Подготовка учебных материалов на основе кода программы.						
Подготовка описания разработанного программного продукта и презентации для участия проекта в конкурсах.						

Входная информация

Для отправителя	Для получателя
• секретная информация • открытый ключ	• зашифрованное сообщение • закрытый ключ



Выходная информация

Для отправителя	Для получателя
• зашифрованное сообщение	• расшифрованное сообщение

Правовое обеспечение

- Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 N 149-ФЗ
- Приказ ФСБ РФ от 9 февраля 2005 г. N 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»

Математическое обеспечение

- теоремы об общем наибольшем делителе двух чисел и мультипликативно обратном элементе
- расчет открытого ключа: $n_i = (W*n_i^s) \bmod M$
- формула зашифровки сообщения: $Ci = n_1*x_{(i-1)k+1)} + n_2*x_{(i-1)k+2)} + \dots n_k*x_{ik}$
- формулы шифра Виженера: $C_i = (P_i + K_i\ ) \bmod M$ $P_i = (C_i - K_i\ + M) \bmod M$
- формула для дешифровки: $C_i^s = (W^{-1}*c_i) \bmod M$

Машинная реализация задачи

Аппаратное обеспечение	Программное обеспечение
• ЦПУ: 1 ГГц или выше ОЗУ: 512 МБ или выше	• Windows 7 / 8 / 10 • Python

Криптосистема с открытым ключом на основе задачи рюкзака

Теория | Расчет открытого ключа | Зашифровка сообщения | Расшифровка сообщения | О программе

Введите элементы супервозрастающей последовательности
или нажмите кнопку RANDOM

Первый элемент 5

Второй элемент 19

Третий элемент 41

Четвертый элемент 100

Пятый элемент 228

Шестой элемент 460

Седьмой элемент 884

Восьмой элемент 1810

Введите кодовое число M
превышающее сумму всех элементов 3589

Рассчитать открытый ключ

Полученное число W 2378

взаимно простое с M 3589

Найденное число iW 1876

мультипликативно обратное к W 2378

Сохранить открытый ключ

1123 2114 595 926 245 2824 2587 969

Сохранить закрытый ключ

Криптосистема с открытым ключом на основе задачи рюкзака

Теория | Расчет открытого ключа | Зашифровка сообщения | Расшифровка сообщения | О программе

Введите открытый ключ

1123 2114 595 926 245 2824 2587 969

Введите сообщение

Пример секретного сообщения

Зашифрованное сообщение

4946 2366 8631 8630 2249 8759 8098 4786 7495
4907 2327 5036 2693 5647 480 86 4009 3348 36
3959 7882 4901 2270 4979 7933 5108 2485 9089

Загрузить из файла

Зашифровать сообщение

Сохранить шифровку

Шифрование завершено!

2485 5108 7933 4979 2270 4901 7882
3959 36 3348 4009 86 480 5647 2693
5036 2327 4907 7495 4786 8098 8759
2249 8630 8631 2366 4946 6467 6265
2954 2709 6459 6109 3923 3923 5778
8429 3923 8696 3923 2954 6747 2709
6510 6502 2709 5778 8429 6510 2709
9089 6265 6510 4946 ['0', '1', '0', '0', '1',
'0', '1', '0'] ['0', '1', '1', '0', '1', '0', '1', '1'] ['0',
'1', '1', '0', '0', '0', '1', '1'] ['0', '1', '1', '0', '0',
'1', '1', '1'] ['0', '1', '1', '0', '0', '0', '0', '0'] ['0',
'1', '1', '0', '1', '0', '1', '1'] ['1', '0', '0', '1', '0',
'1', '1', '1'] ['0', '1', '1', '0', '1', '1', '0', '0'] ['0',
'1', '1', '0', '0', '0', '0', '0'] ['0', '1', '1', '0', '0',
'1', '0', '1'] ['0', '1', '1', '0', '1', '0', '1', '1'] ['0',
'1', '1', '0', '0', '0', '0', '0'] ['0', '1', '1', '0', '1',
'1', '0', '1'] ['0', '1', '1', '0', '1', '0', '0', '0'] ['0',
'1', '1', '0', '1', '0', '0', '1'] ['0', '1', '0', '1', '1',
'1', '1', '0'] ['0', '1', '1', '0', '1', '0', '0', '1'] ['1',
'0', '0', '1', '0', '1', '1', '1'] ['0', '1', '1', '0', '1',
'1', '0', '0'] ['0', '1', '1', '0', '1', '0', '0', '1'] ['0',
'1', '1', '0', '1', '0', '0', '1'] ['0', '1', '0', '1', '1',
'1', '0', '0'] ['0', '1', '1', '1', '0', '1', '0', '0'] ['0',
'1', '1', '0', '0', '0', '0', '0'] ['0', '1', '1', '0', '1',
'0', '0', '0'] ['0', '1', '1', '0', '0', '0', '1', '1'] ['0',

Криптосистема с открытым ключом на основе задачи рюкзака

Теория | Расчет открытого ключа | Зашифровка сообщения | Расшифровка сообщения | О программе

Введите закрытый ключ

5 19 41 100 228 460 884 1810 3589 2378 1876

Введите зашифрованное сообщение

4946 2366 8631 8630 2249 8759 8098 4786 7495
4907 2327 5036 2693 5647 480 86 4009 3348 36
3959 7882 4901 2270 4979 7933 5108 2485 9089

Расшифрованное сообщение

Пример секретного сообщения

Загрузить из файла

Загрузить из файла

Расшифровать сообщение

Сохранить сообщение

Расшифровка завершена!

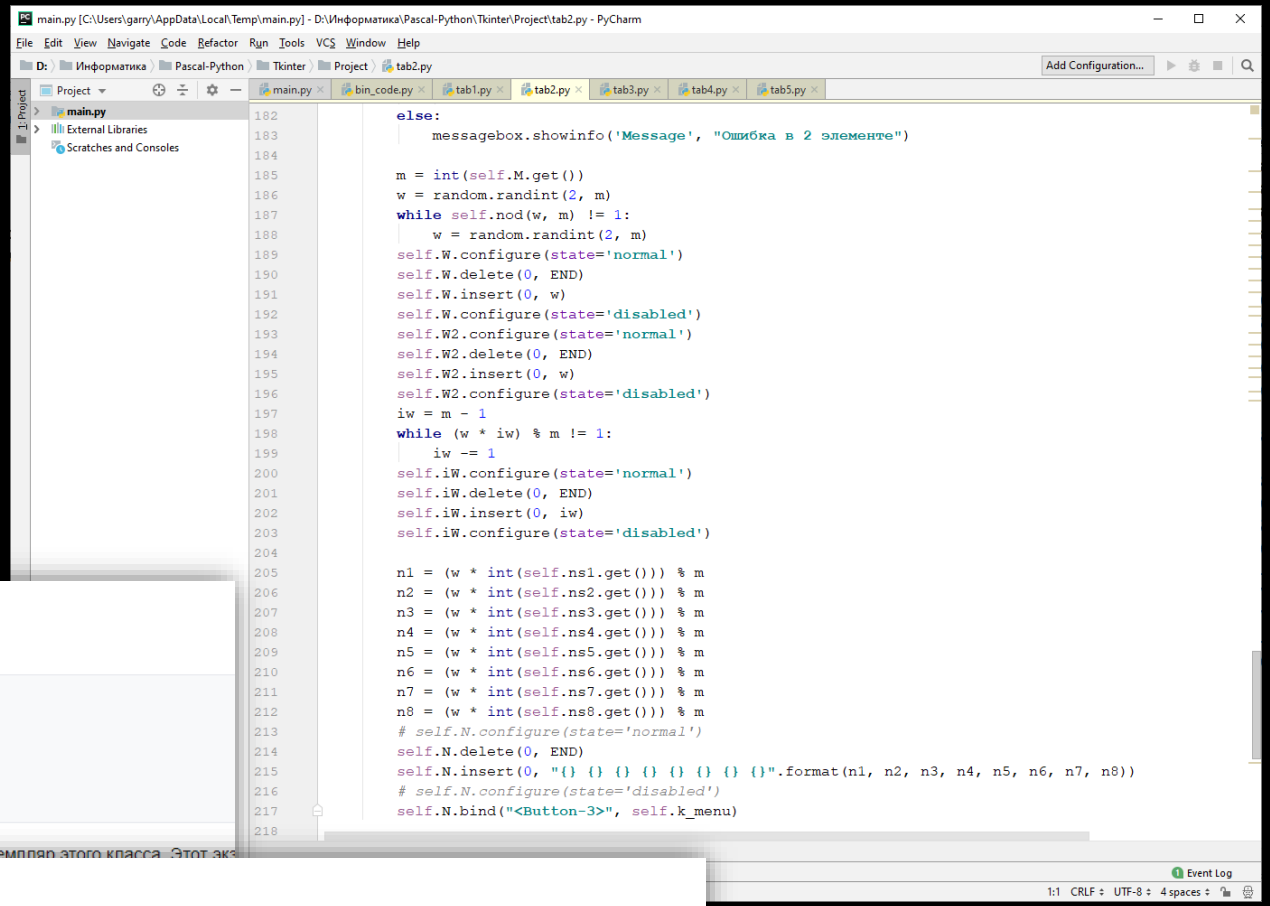
яинещбоос огонтеркес ремирП['0', '1', '1', '1', '1', '0', '1', '0'] ['0', '1', '1', '0', '0', '0', '1', '1'] ['0', '1', '1', '0', '1', '0', '0', '0'] ['0', '1', '1', '0', '0', '0', '0', '0'] ['0', '1', '1', '1', '0', '1', '0', '0'] ['0', '1', '0', '1', '1', '1', '0', '0'] ['0', '1', '1', '0', '1', '0', '0', '1'] ['0', '1', '1', '0', '1', '0', '0', '1'] ['0', '1', '1', '0', '1', '1', '0', '0'] ['1', '0', '0', '1', '0', '1', '1', '1'] ['0', '1', '1', '0', '1', '0', '0', '1'] ['0', '1', '0', '1', '1', '1', '1', '0'] ['0', '1', '1', '0', '1', '0', '0', '1'] ['0', '1', '1', '0', '1', '0', '0', '0'] ['0', '1', '1', '0', '1', '1', '0', '1'] ['0', '1', '1', '0', '0', '0', '0', '0'] ['0', '1', '1', '0', '1', '0', '1', '1'] ['0', '1', '1', '0', '0', '1', '0', '1'] ['0', '1', '1', '0', '0', '0', '0', '0'] ['0', '1', '1', '0', '1', '1', '0', '0'] ['1', '0', '0', '1', '0', '1', '1', '1'] ['0', '1', '1', '0', '1', '0', '1', '1'] ['0', '1', '1', '0', '0', '1', '1', '1'] ['0', '1', '1', '0', '1', '0', '1', '1'] ['0', '1', '0', '0', '1', '0', '1', '0'] 1272 2754 288 60 620 807 2098 2098 748 3259 2098 1691 2098 288 2558 60 2982 2330 60 748 3259 2982 60 3214 2754 2982 1131 4946 6510 6265 9089 2709 6510 8429 5778 2709 6502 6510 2709 6747 2954 3923 8696 3923 8429 5778

Подготовка учебных материалов на основе кода программы

Основные классы

Модуль tkinter включает следующие классы:

1. **Button** (кнопка)
2. **Radiobutton** (радио-кнопка)
3. **Checkbutton** (флажок)
4. **Entry** (однострочное поле для ввода)
5. **Text** (многострочное поле для ввода)
6. **Label** (метка)
7. **Scale** (ползунок)
8. **Scrollbar** (полоса прокрутки)
9. **Frame** (виджет для группировки других виджетов)
10. **LabelFrame** (аналог Frame, только с заголовком)
11. **Listbox** (список)
12. **Canvas** (поле для рисования)
13. **PanedWindow** (элемент разделения окна)
14. **Menu** (главное меню)
15. **Tk** (главное единственное окно)
16. **Toplevel** (дочернее окно)



Button

Виджет Button - самая обыкновенная кнопка, которая используется в тысячах программ. Пример кода:

```
from Tkinter import *
root=Tk()
button1=Button(root,text='ok',width=25,height=5,bg='black',fg='red',font='arial 14')
button1.pack()
root.mainloop()
```

Разберем этот небольшой код. За создание, собственно, окна, отвечает класс Tk(), и первым делом нужно создать экземпляр этого класса. Этот экз
вы можете назвать его

- text - какой текст бу
- width,height - соотв
- bg - цвет кнопки (со
- fg - цвет текста на
- font - шрифт и его р

Далее, нашу кнопку не
Пока, чтобы размести
окно не будет создано

Label

Label - это виджет, предназначенный для отображения какой-либо надписи без возможности редактирования пользователем. Имеет те же свойства
кнопки.

Entry

Entry - это виджет, позволяющий пользователю ввести одну строку текста.

- **borderwidth** - ширина бордюра элемента
- **bd** - сокращение от **borderwidth**
- **width** - задаёт длину элемента в знакоместах.
- **show** - задает отображаемый символ.

Text

Text - это виджет, который позволяет пользователю ввести любое количество текста. Имеет дополнительное свойство wrap, отвечающее за перенос
словам, нужно использовать значение WORD).Например:

```
from Tkinter import *
root=Tk()
text1=Text(root,height=7,width=7,font='Arial 14',wrap=WORD)
text1.pack()
root.mainloop()
```

Результат проекта:

Разработанное программное обеспечение может выступать в роли дополнительного учебного материала по теме информационной безопасности, а также в рамках изучения создания графических приложений.

Создание таких обучающих программ становится особенно актуальным в связи с проведением в 2020 - 2022 годах эксперимента по внедрению целевой модели цифровой образовательной среды.

Таким образом, цель данного проекта созвучна с теми приоритетными задачами, которые поставлены перед школой в настоящее время – повышение доступности качественного образования.

Свидетельство о государственной регистрации программы для ЭВМ – см. по ссылке

Дальнейшее развитие проекта:

- ✓ создание веб-версии программы для размещения ее в открытом доступе;
- ✓ создание англоязычной версии для расширения аудитории сайта;
- ✓ размещение обучающей программы в виде приложения в МЭШ;
- ✓ информационная методическая поддержка (проведение вебинаров, запись обучающих видеороликов)